SolarWinds Failover Engine v6.7

Command Line Installation

solarwinds

SolarWinds Failover Engine

Copyright© 1995-2013 SolarWinds, Inc., all rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds®, the SolarWinds logo, ipMonitor®, LANsurveyor®, and Orion® are among the trademarks or registered trademarks of the company in the United States and/or other countries. All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft®, Windows 2000 Server®, Windows 2003 Server®, and Windows 2008 Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

Fluent is a trademark of Microsoft Corporation and the Fluent user interface is licensed from Microsoft Corporation.

SolarWinds Failover Engine version 6.7.0 [Build 10738] 2.28.2013

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	1.866.530.8100 www.solarwinds.com
Technical Support	www.solarwinds.com/support
User Forums	http://support.solarwinds.net/support **Note:** You need a customer account to access the Customer Support area of the website.

SolarWinds Failover Engine Documentation Library

The following documents are included in the SolarWinds Failover Engine documentation library:

Document	Purpose
Administrator Guide	Provides detailed configuration and conceptual information.
Installation Guides	Provides detailed setup information.
Page Help	Provides help for every window in the SolarWinds Failover Engine user interface.
Release Notes	Provides late breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com/

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items including buttons and fields.
Italics	Book and CD titles, variable names, new terms.
`Fixed font`	File and directory names, commands and code examples, text typed by you.
Straight brackets, as in [*value*]	Optional command parameters
Curly braces, as in {*value*}	Required command parameters
Logical OR, as in *value1*|*value2*	Exclusive command parameters where only one of the options can be specified.

Contents

Chapter 1:
Introduction....7
SolarWinds Failover Engine Concepts....7
Communications....8
SolarWinds Failover Engine Switchover and Failover Processes....10

Chapter 2:
Implementation....11
Implementation Overview....11
Common Requirements....11
Server Architecture Options....13
Virtual to Virtual (V2V)....13
Physical to Virtual (P2V)....13
Physical to Physical (P2P)....14
Cloning Technology Options....15
Supported Pre-Clone Technologies....15
Supported Install Clone Technologies....15
Network Options....16
Local Area Network (LAN)....16
Wide Area Network (WAN)....17
Network Interface Card (NIC) Configuration....18
Firewall Configuration Requirements....20
Anti-Malware Recommendations....21

Chapter 3:
Command Line Installation....23
Command Line Usage....23
Parameter File Elements....24
Command Line Installation of the Primary Server....26
Command Line Installation of a Virtual Secondary Server....27
Command Line Installation of a Physical Secondary Server....28
Post Installation Configuration....28
Configure actions to take upon failure of a service....29
When Additional Pollers (AP)s are not installed, create an Exclusion Filter.31
When IPAM 2.0 is installed, create an Inclusion Filter....31

Command Line Installation of SolarWinds Failover Engine Client Tools.....31

Command Line Uninstall of SolarWinds Failover Engine 32

Appendix A:

Setup Error Messages.....35

Appendix B:

Installation Verification Testing.....41

Testing a SolarWinds Failover Engine Pair.....41

Exercise 1 - Auto-switchover.....41

Exercise 2 - Data Verification.....43

Exercise 3 - Switchover.....44

Glossary.....47

Chapter 1

Introduction

SolarWinds Failover Engine is a Windows based service specifically designed to provide High Availability or Disaster Recovery protection for SolarWinds Server configurations without requiring any specialized hardware.

SolarWinds Failover Engine Concepts

Architecture

SolarWinds Failover Engine software is installed on a *Primary* (production) server and a *Secondary* (ready-standby) server. These names refer to the Identity of the servers and never change throughout the life of the server.

Note: In this document, the term “Cluster” refers to a SolarWinds Failover Engine Cluster. Refer to the *Glossary* for more information about SolarWinds Failover Engine Clusters.

Depending on the network environment, SolarWinds Failover Engine can be deployed in a Local Area Network (LAN) for High Availability or Wide Area Network (WAN) for Disaster Recovery, providing the flexibility necessary to address most network environments.

When deployed, one of the servers performs the *Role* of the *Active* server that is visible on the Public network while the other is *Passive* and hidden from the Public network but remains as a ready-standby server. The secondary server has the same domain name, uses the same file and data structure, same Principal (Public) network address (in a LAN), and can run all the same applications and services as the primary server. Only one server can display the Principal (Public) IP address and be visible on the Public network at any given time. SolarWinds Failover Engine software is symmetrical in almost all respects, and either the primary server or the secondary server can take the active role and provide protected applications to the user.

SolarWinds Failover Engine provides continuous access to the passive server simultaneously as the active server continues to service clients allowing the passive server to be easily accessed for maintenance purposes, updating anti-malware definition files, receiving operating system hot-fixes, updates and patches from third-party management software, and allows use of third-party monitoring tools.

Protection Levels

SolarWinds Failover Engine provides the following protection levels:

- *Server Protection* – provides continuous availability to end users through a hardware failure scenario or operating system crash. Additionally, SolarWinds Failover Engine protects the network identity of the production server, ensuring users are provided with a replica server on the failure of the production server.
- *Network Protection* – proactively monitors the network by polling up to three nodes to ensure that the active server is visible on the network.
- *Application Protection* – maintains the application environment ensuring that applications and services stay alive on the network.
- *Performance Protection* – monitors system performance attributes to ensure that the system administrator is notified of problems and can take pre-emptive action to prevent an outage.
- *Data Protection* – intercepts all data written by users and applications, and maintains a copy of this data on the passive server which can be used in the event of a failure.

SolarWinds Failover Engine provides all five protection levels continuously, ensuring all facets of the user environment are maintained at all times, and that the Public network continues to operate through as many failure scenarios as possible.

Communications

SolarWinds Failover Engine communications consist of two crucial components, the SolarWinds Channel and the Principal (Public) network.

To accommodate communications requirements, SolarWinds Failover Engine can be configured to use either multiple NICs (1 X Channel and 1 X Principal (Public) connection) on each server providing a separate dedicated SolarWinds Channel network from the Principal (Public) network or a single NIC on each server to fulfill both the SolarWinds Channel and Principal (Public) network connection requirements.

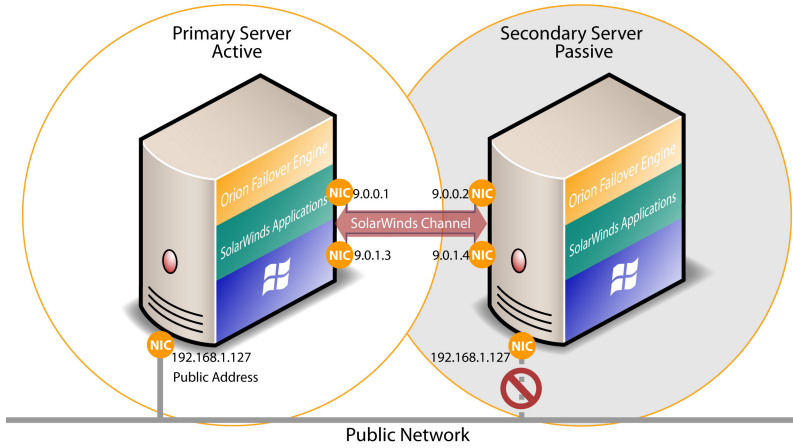

Figure 1: Communications Between primary and secondary Servers

SolarWinds Channel

The first component is the SolarWinds Channel which provides communications between the active and passive servers. The SolarWinds Channel is used for control and data transfer from the active server to the passive server and for monitoring of the active server's status by the passive server.

The NICs on the active and passive servers used for the SolarWinds Channel are normally configured with IP addresses outside of the Principal (Public) network subnet range and are referred to as the SolarWinds Channel addresses. During installation, setup will disable NetBIOS for the SolarWinds Channel(s) on the active and passive servers to prevent server name conflicts.

The NICs that support connectivity across the SolarWinds Channel can be standard 100BaseT Ethernet cards providing a throughput of 100 Mbits per second across standard Cat-5 cabling. When using multiple NICs providing a separate dedicated SolarWinds Channel, this channel requires no hubs or routers, but the direct connection does require crossover cabling.

When configured for a WAN deployment, configure the SolarWinds Channel to use static routes over switches and routers to maintain continuous communications independent from corporate or public traffic.

Principal (Public) Network

The second component is the Principal (Public) network used by clients to connect to the active server. The Principal (Public) network provides access to the Principal (Public) IP address used by clients to connect to the active server.

The Principal (Public) IP address is a static IP address that is only available on the currently active server and is the IP address a client uses to connect to the

active server. It must be configured as a static IP address, that is, not DHCP (Dynamic Host Configuration Protocol) enabled. In the figure above, the IP address is configured as `192.168.1.127`. The Principal (Public) IP address is shared by the active and passive servers in a LAN and is always available on the currently active server in the cluster. In the event of a switchover or failover, the Principal (Public) NIC is blocked on the previously active server and is then available on the new active server. When configured, a Management IP address will provide access to a server regardless of the role of the server.

Management IP Address

All servers in the cluster can be configured with Management IP addresses that allow access to the server when the server is in the passive role. The Management IP address is a static IP address in the same subnet as the Principal (Public) IP address and is always available for administrators to access the server.

SolarWinds Failover Engine Switchover and Failover Processes

SolarWinds Failover Engine uses four different procedures – managed switchover, automatic switchover, automatic failover, and managed failover – to change the role of the active and passive servers depending on the status of the active server.

- *Managed Switchover* – You can click **Make Active** on the SolarWinds Failover Manager *Server: Summary* page to manually initiate a managed switchover. When a managed switchover is triggered, the running of protected applications is transferred from the active machine to the passive machine in the server pair. The server roles are reversed.
- *Automatic Switchover* – Automatic switchover (auto-switchover) is similar to failover (discussed in the next section) but is triggered automatically when system monitoring detects failure of a protected application.
- *Automatic Failover* – Automatic failover is similar to automatic switchover (discussed above) but is triggered when the passive server detects that the active server is no longer running properly and assumes the role of the active server.
- *Managed Failover* – Managed failover is similar to automatic failover in that the passive server automatically determines that the active server has failed and can warn the system administrator about the failure, but no failover actually occurs until the system administrator manually triggers this operation (the default configuration in a DR environment).

Chapter 2

Implementation

This chapter discusses the deployment options and prerequisites to successfully implement SolarWinds Failover Engine and provides a step-by-step process to assist in selecting options required for installation.

Implementation Overview

SolarWinds Failover Engine is a versatile solution that provides multiple configurations to suit user requirements. SolarWinds Failover Engine can be deployed as a Pair in either a LAN or WAN.

This chapter discusses the deployment options and the necessary prerequisites for each option, and provides a step-by-step process to assist you in selecting the options required to successfully implement SolarWinds Failover Engine.

Prior to installing SolarWinds Failover Engine, you must identify the preferred deployment options. The installation process requires you to select options throughout the procedure to achieve the best configuration for your requirements.

During the installation process, SolarWinds Failover Engine performs a variety of checks to ensure the server meets the minimum requirements for a successful installation. If the server fails one of the checks, a *Critical Stop* or *Warning* message is displayed. *Setup Error Messages* provides an explanation of the messages. You must resolve Critical Stops before you can proceed with setup.

Common Requirements

The following requirements must be met to support a successful installation of SolarWinds Failover Engine.

Environmental Prerequisites

The server protected by SolarWinds Failover Engine must not be configured as a domain controller, global catalog, or DNS server. If it is, it must be reconfigured before installing SolarWinds Failover Engine.

System Requirements

To support the installation of SolarWinds Failover Engine, systems must meet the following minimum requirements:

- Supported Operating Systems

Important: SolarWinds Failover Engine requires that Microsoft™ .Net Framework 4 be installed prior to running `Setup.exe`. If .Net Framework 4 is not installed when you attempt to initiate Setup, SolarWinds Failover Engine will prevent installation until .Net Framework 4 is installed.

Windows Server 2003 must have Windows Imaging Component (WIC) installed prior to installing Microsoft .Net Framework 4.

- Windows Server 2003 x86 and x64 Standard / Enterprise / R2 with SP2
- Windows Server 2008 x 86 and x64 Standard / Enterprise with SP1 or SP2
- Windows Server 2008 R2 x64 Standard / Enterprise / Datacenter and SP1
- Windows Server 2012 x64 Standard / Datacenter

- 1GB of available RAM (2GB recommended)

Note: During the setup process, SolarWinds Failover Engine verifies that a minimum of 1GB of RAM is available.

To ensure proper operation, SolarWinds Failover Engine requires a minimum of 1GB of RAM in addition to the memory requirements of the Operating System and installed applications. 256MB of RAM must remain available to the SolarWinds Failover Engine application suite at all times.

- 2 GB of disk space available on the drive to receive the SolarWinds Failover Engine installation

Note: Although SolarWinds Failover Engine requires only 2GB of available disk space on the drive to receive the SolarWinds Failover Engine installation, once installed, the size of each send and receive queue is configured by default for 10GB. You must ensure that sufficient disk space is available to accommodate the send and receive queues or modify the queue size configuration to prevent MaxDiskUsage errors.

- Latest Microsoft security updates
- Local administrator rights for installation

Note: SolarWinds Failover Engine services are required to be run under the Local System account.

Configuration Requirements

In addition to the system requirements listed above, the network environment must meet the following criteria to support the installation and operation of SolarWinds Failover Engine:

- Plugs-ins on pre-cloned servers must be located with the same path as on the primary server for a successful installation. For example, if the path on the primary server is `C:\temp\<pluginname.dll>`, then the path to the plug-in on the pre-cloned server(s) also must be `C:\temp\<pluginname.dll>`.
- All applications intended to receive SolarWinds Failover Engine protection must be installed and configured on the primary server prior to installing SolarWinds Failover Engine
- The primary and secondary servers must be set to identical System Date, Time, and Time Zone. Once configured, do not change the Time Zone
- If installing on Windows Server 2003, verify that the Principal (Public) network adapter is listed as the first network adapter in the Network Connections Bind Order on each server. (**Network Connections** > **Advanced** > **Advanced Settings**)

Server Architecture Options

SolarWinds Failover Engine supports Virtual to Virtual, Physical to Virtual, and Physical to Physical architectures. The selected server architecture determines the hardware requirements and impacts the technique used to clone the primary server.

Virtual to Virtual (V2V)

In a V2V architecture, SolarWinds Failover Engine allows cloning of the primary server prior to the installation of SolarWinds Failover Engine using VMware Converter, VMware vCenter Cloning Utility, and other 3rd party utilities. Benefits to this architecture include reduced hardware cost, shorter installation time, and use of the Pre-Clone technique for installation. The secondaryvirtual machine must meet the following minimum requirements:

- The configuration of secondary virtual machine must match the primary virtual machine:
  - Similar CPU, including resource management settings
  - Similar memory configuration, including resource management settings.
- Appropriate resource pool priorities
- Each virtual machine in a V2V configuration must be on a separate host to guard against failure at the host level
- Each virtual NIC must use a separate virtual switch (network)

Physical to Virtual (P2V)

P2V architecture is used when the environment requires a mix of physical and virtual machines, such as when SolarWinds Failover Engine is installed on a physical server in an environment with limited available hardware. This architecture is appropriate if you must avoid adding additional physical servers

or when you prefer to migrate to virtual technologies over a period of time. The secondary virtual machine must meet the following minimum requirements:

- The configuration of secondary virtual machine must match the primary physical server:
  - Similar CPU
  - Similar memory
- The secondary virtual machine requires sufficient priority in resource management settings so that other virtual machines do not impact its performance.
- Each virtual NIC must use a separate virtual switch.

Physical to Physical (P2P)

P2P architecture is used in an environment that requires physical servers. Use of P2P architecture requires use of the Install Clone technique.

Primary Server

The primary server in a P2P architecture must meet the hardware and software requirements specified in *Common Requirements*.

Secondary Server

The secondary server in a P2P architecture must meet specific hardware and software requirements to ensure adequate performance when the server assumes the active role.

Hardware

The secondary server in a P2P architecture must meet the following hardware requirements:

- Hardware must be equivalent to the primary server:
  - Similar CPU
  - Similar memory
- An identical number of NICs to the primary server
- Drive letters must match the primary server
- The amount of available disk space on each partition should be equal to or greater than that on the equivalent partition on the primary server
- ACPI compliance must match the primary server

Note: The SolarWinds Failover Engine standard implementation process assumes that the Advanced Configuration and Power Interface (or ACPI) compliance of both machines are identical. If this is not the case, contact SolarWinds Support at *http://www.solarwinds.com/support* for further information.

Software

The secondary server in a P2P architecture must meet the following software requirements:

- The OS version and Service Pack version must match the primary server
- The OS Updates installed must match the primary Server
- The OS must be installed to same driver letter and directory as on the primary server
- The machine name must be different from the primary server prior to installing SolarWinds Failover Engine
- Set up in a Workgroup prior to installing SolarWinds Failover Engine
- The System Date, Time, and Time Zone must be consistent with primary server

Cloning Technology Options

Cloning the primary server to create a nearly identical secondary server involves different techniques depending on the selected server architecture option.

Supported Pre-Clone Technologies

The following cloning technologies are supported for creating Pre-Cloned images for use as a secondary server:

- VMware Converter for Physical to Virtual (P2V)
- VMware vCenter virtual machine cloning for Virtual to Virtual (V2V)
- Other third party utilities

Supported Install Clone Technologies

Installation of SolarWinds Failover Engine provides support for NTBackup on Windows 2003 and Wbadmin on Windows Server 2008 for automated Install Cloning.

This process is automated, but all prerequisites for the secondary server specified under *Physical to Physical (P2P)* requirements must be met.

Note: When installing in a Physical to Virtual (P2V) architecture, VMware Tools must not be installed on the secondary server during the SolarWinds Failover Engine installation process. If VMware Tools are currently installed on the secondary server, you must fully uninstall VMware Tools prior to initiation of the Setup process. Once the installation of SolarWinds Failover Engine has completed, you may reinstall VMware Tools.

Important: When installing on Windows Server 2003, verify that the Principal (Public) network adapter is listed first in the bind order of the **Network Connections** > **Advanced** > **Advanced Settings** dialog.

Network Options

Networking requirements are contingent upon how SolarWinds Failover Engine is deployed. To deploy as a High Availability (HA) solution, a LAN configuration is required. To deploy SolarWinds Failover Engine for Disaster Recovery (DR), a WAN configuration is required. Each network configuration has specific configuration requirements to ensure proper operation.

Note: SolarWinds recommends that the SolarWinds Channel be configured on a different subnet than the Principal (Public) network. In the event that this is not possible, see SWREFID-2528 — Configuring SolarWinds Channel and Public Connections to use the Same Subnet.

SolarWinds Failover Engine can be configured to run using multiple NICs or a single NIC.

Multiple NICs

SolarWinds Failover Engine supports use of multiple NICs on each server pair. When using multiple NICs, one NIC is configured with the Principal (Public) IP address for client access while a second dedicated NIC is configured with the SolarWinds Channel IP address. Deploying with multiple NICs provides the advantage of redundancy and also removes the risk of single point of failure that exists in single NIC configurations. To configure using multiple NICs on each server, see *Multi-NIC Configuration*.

Note: SolarWinds Failover Engine does NOT out-of-the-box support teams of NICs but can be configured to support teamed NICs with additional configuration steps when installing with teamed NICs present. See knowledge base article SWREFID-1947 — How to Install the SolarWinds Failover Engine Packet Filter Driver on a NIC team (Teamed NICs, NIC Teaming) for more information about teamed NICs.

Single NIC

SolarWinds Failover Engine also supports use of a single NIC configured to perform both functions, providing the Principal (Public) IP address to users and the SolarWinds Channel for data transfer and control. To configure using a single NIC on each server, see *Single NIC Configuration*.

Local Area Network (LAN)

When deployed in a LAN environment, SolarWinds Failover Engine requires that both servers use the same Principal (Public) IP address. Each server also requires a SolarWinds Channel IP address.

Wide Area Network (WAN)

SolarWinds Failover Engine supports sites with different subnets. In this scenario, the primary and secondary servers in the SolarWinds Failover Engine Pair will require unique Principal (Public) IP addresses in each subnet and a unique SolarWinds Channel IP address in each subnet for each server . During Setup, select the *Use different IP addresses for Secondary (Recommended for DR secondary)* and specify the Principal (Public) IP addresses of both the secondary server and the primary server in the pair.

SolarWinds Failover Engine , using multiple NICs, also supports sites with the same subnet. In this scenario the SolarWinds Failover Engine shares a single Principal (Public) IP address between the primary and secondary server making it available on the active server. Although the SolarWinds Channel addresses should be unique within the same subnet. During Setup, select the *Use same IP addresses for Secondary (Recommended for HA secondary)* on the *Principal (Public) IP Address Configuration* page and specify the IP address to be shared by both servers.

WAN Requirements

WAN deployments require the following:

- Persistent static routing configured for the channel connection(s) where routing is required
- One NIC minimum, two NICs (1 x Public and 1 x Channel) are recommended
- At least one Domain Controller at the Disaster Recovery (DR) site
- If the Primary and DR site uses the same subnet:
  - During install, follow the steps for a LAN or VLAN on the same subnet
  - Both the primary and secondary servers in the pair use the same Public IP address
- If the Primary and DR site use different subnets:
  - During install, follow the steps for a WAN
  - The primary and secondary servers in the SolarWinds Failover Engine pair require a separate Principal (Public) IP address and a SolarWinds Channel IP address
  - Provide a user account with rights to update DNS using the `DNSUpdate.exe` utility provided as a component of SolarWinds Failover Engine through SolarWinds Failover Manager **Applications** > **Tasks** > **User Accounts**
  - SolarWinds recommends integrating Microsoft DNS into AD so that `DNSUpdate.exe` can identify all DNS Servers that require updating

- At least one Domain Controller at the DR site
- Refer to the following articles in the SolarWinds Knowledge Base:
  - Knowledge base article SWREFID-1937 – Configuring DNS with SolarWinds Failover Engine in a WAN Environment
  - Knowledge base article SWREFID-1938 – Configuring SolarWinds Failover Engine to Update BIND9 DNS Servers Deployed in a WAN

Bandwidth

SolarWinds Failover Engine includes automatic bandwidth optimization in WAN environments. This feature compresses data transferred over the SolarWinds Channel, optimizing the traffic for low bandwidth connections causing some additional CPU load on the active server.

Determine the available bandwidth and estimate the required volume of data throughput to determine acceptable latency for the throughput. Additionally, the bandwidth can affect the required queue size to accommodate the estimated volume of data. SolarWinds recommends making a minimum of 1Mbit of spare bandwidth available to SolarWinds Failover Engine.

Latency

Latency has a direct effect on data throughput. Latency on the link should not fall below the standard defined for a T1 connection (2-5ms for the first hop).

SolarWinds Failover Engine Diagnostics can assist in determining the available bandwidth, required bandwidth, and server workload. For more information about SolarWinds Failover Engine Diagnostics, contact SolarWinds Professional Services.

Network Interface Card (NIC) Configuration

SolarWinds Failover Engine supports the use of both a single NIC or multiple NIC configuration on primary and secondary servers. The number of NICs present will determine how the NICs are configured.

Important: The primary and secondary servers must have the same number of NICs.

Multi-NIC Configuration

When Using multiple NICs, one NIC functions for client and management access while a second NIC functions as a dedicated SolarWinds Channel.

Primary Server

The primary server is configured with the following connections:

- A Principal (Public) network connection configured with a static Principal (Public) IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.
- SolarWinds Channel connection(s) configured with a static IP address in a different subnet than the Principal (Public) IP address, and with a different IP address than the secondary server channel NIC, and network mask. No gateway or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared on the SolarWinds Channel connection(s) prior to installing SolarWinds Channel.

Secondary Server

The secondary server must have the same number of NICs as the primary server and is configured as follows:

- A Principal (Public) connection configured with a static IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.

  Note: If deploying in a WAN, the Principal (Public) IP address of the secondary server may be in a different subnet than the primary server.

- SolarWinds Channel network connection(s) configured on a separate dedicated NIC with a static IP address in a different subnet than the secondary Principal (Public) IP address, and with a different IP address than the primary server's SolarWinds Channel NIC, and a network mask. No gateway address or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared on the SolarWinds Channel connection(s) prior to installing SolarWinds Channel.

Single NIC Configuration

Configuring SolarWinds Channel using a single NIC requires that both functions (Client access and Channel operations) use the same physical or virtual NIC.

Primary Server

The primary server requires a single NIC configured with the following IP addresses:

- A Principal (Public) IP address - configured using a static IP address, network mask, gateway address, preferred DNS server address, and secondary (if applicable) DNS server address.

- A SolarWinds Channel IP address - configured on the same NIC as the Principal (Public) IP address configured with a static IP address in a different subnet than the Principal (Public) IP address, and a network mask. No gateway address or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared prior to installing SolarWinds Channel.

  Important: Ensure that your server has a persistent DNS entry in the DNS system for the Principal (Public) IP address.

Secondary Server

The secondary server must have the same number of NICs as the primary server and be configured as follows:

- A SolarWinds Channel IP address - configured with a static IP address and the network mask. No gateway or DNS server address is configured. NetBIOS will be disabled during the installation process to prevent server name conflicts.
- The *Register this connection's addresses in DNS* check box must be cleared prior to installing SolarWinds Channel.

  Important: Ensure that your server has a persistent DNS entry in the DNS system for the Principal (Public) IP address. The secondary server's Principal (Public) IP address will be configured during the Setup process.

Firewall Configuration Requirements

When firewalls are used to protect networks, you must configure them to allow traffic to pass through both the *Client Connection port* (`52267`) and the *Default Channel port* (`57348`).

SolarWinds recommends that the firewall be configured to allow the Client to connect to the Client Connection port by process, `nfgui.exe`, rather than by a specific port. To enable Channel communications between servers, configure the firewall to allow traffic to pass through on Port `57348`, the Default Channel port.

Important: When installing on Windows Server 2008 or 2012, Microsoft Windows may change the connection type from a Private network to an Unidentified network after you have configured the firewall port to allow channel communications resulting in the previously configured firewall changes to be reset for the new network type (Unidentified).

The firewall rules must be recreated to allow traffic to pass through for the Client Connection port and the Default Channel port. SolarWinds recommends that the firewall be configured to allow the Client to connect to the Client Connection port by process, `nfgui.exe`, rather than by a specific port. To enable Channel communications between servers, change the Network List Manager Policy so that the SolarWinds Channel network is identified as a Private Network, and not the default Unidentified Network, and configure the firewall to allow traffic to pass through on Port `57348`, the Default Channel port.

Anti-Malware Recommendations

Consult with and implement the advice of your anti-malware provider, as SolarWinds guidelines often follow these recommendations. Consult the SolarWinds Knowledge Base for up to date information on specific anti-malware products.

Do not use file level anti-malware to protect application server databases, such as MS SQL Server databases. The nature of database contents can cause false positives in malware detection, leading to failed database applications, data integrity errors, and performance degradation.

SolarWinds recommends that when implementing SolarWinds Failover Engine, you do not replicate file level anti-malware temp files using SolarWinds Failover Engine.

The file level anti-malware software running on the primary server must be the same as the software that runs on the secondary server. In addition, the same file level anti-malware must run during both active and passive roles.

Configure file level anti-malware to use the Management IP address on the passive server for malware definition updates. If this is not possible, manually update malware definitions on the passive server.

Exclude the following SolarWinds directories from file level anti-malware scans (`C:\Program Files\SolarWinds\FoE\` is the default installation directory):

- `C:\Program Files\SolarWinds\FoE\r2\logs`
- `C:\Program Files\SolarWinds\FoE\r2\log`

Any configuration changes made to a file level anti-malware product on one server (such as exclusions) must be made on the other server as well. SolarWinds Failover Engine does not replicate this information.

Chapter 3

Command Line Installation

The following provides the procedures to install SolarWinds Failover Engine from the command line including all available parameter file elements.

Command Line Usage

To perform an unattended installation, you must run the `start /wait Setup` command with the appropriate parameters from the command line. Additionally, you must create a `.txt` file (parameter file) that contains the information necessary to provide the intended options to the Setup application. The following information provides details about the parameters and parameter file necessary to successfully perform a command line installation.

Note: Users should not cut-and-paste from this .pdf document but should type the actual commands and parameters.

```
start /wait Setup [-h]
[-f<parameter file>] [-ni [-sp -se -sw -di]]
[-DNSPassword:<password>] [-BACKUPPassword:<password>]
[-secondaryInstall|-uninstall|-drvInstall|]
```

Table 1: Command Line Parameters

Parameter	Description
`-h`	Displays this usage information
`-f:<parameter file>`	Uses a file of parameters to run **Important:** If the file name/path contains any white space (space, tab) or special characters(-, /, etc.) then it must be enclosed in quotes "..."
`-ni`	Not interactive, suppresses the Graphical User Interface. This instructs Setup not to use the Graphical User Interface. If this parameter is not specified but a parameter file is specified, the Graphical User Interface pages will be fully populated and require that the **Next** or **Proceed** button be clicked and any popup dialog boxes be acknowledged.
`-sp`	Suppress Progress (Only for Non- interactive)

Parameter	Description
`-se`	Suppress Errors (Only for Non- interactive)
`-sw`	Suppress Warnings (Only for Non- interactive)
`-di`	Display Info (Only for Non- interactive)
`-DNSPassword:<password>`	The password used for DNSUpdate
`-BACKUPPassword:<password>`	The password used for WBADMIN
`-uninstall`	Do not use unless instructed to do so
`-ADMINPassword:<Password>`	The password to use for Administrator
`-drvInstall`	Do not use unless instructed to do so
`-secondaryInstall`	Do not use unless instructed to do so

Important: Only the DOS shell requires the "`start /wait`"

Table 2: Return Codes

Code	Description
`0`	: Success
`1`	: Incorrect Usage (not enough parameters)
`2`	: Invalid Parameter
`3`	: File cannot be opened (file cannot be found)
`4`	: File parse failed
`5`	: Unable to Run (See output for specific problems)
`6`	: Processing failed

Parameter File Elements

The parameter file is used to pass setup options to the Setup application and is made up of a sequence of tagged lines, with the tag indicating what the data describes.

For example: `INSTALLTYPE:Install`

Important: The parser is case insensitive. Any values containing white space must be enclosed with double quotes, for example "pre clone". If the file name/path contains any white space (space, tab) or special characters(-, /, etc.) then it must be enclosed in quotes "..."

Table 3: Parameter File Elements

Tag	Values	Comments
FORMATVERSION:	V1_0 (Default)	Used to indicate the Format of the tags listed after this line. This can be used multiple times.
INSTALLTYPE:	Install Install Client Tools Only Install AM(X) Install Service Pack Uninstall Uninstall Components	
PLUGINPATH:	Must be a valid path and include the plug-in file name	Only one per line but can be defined multiple times
FEATUREFORINSTALLATION:	SolarWinds Failover Engine	Only one per line but can be defined multiple times
SERVERROLE:	Primary Secondary	
TOPOLOGY:	HA DR	
ACCEPT_EULA:	True False	
DEFAULTCHANNELPORT:	Must be an integer	
DESTINATIONPATH:	Must be a valid path	
BACKUPDESTINATIONPATH:	Must be a valid path	Used to indicate where to write the pre-synchronization data
BCKUPSOURCEPATH:	Must be a valid path	Used to locate the pre-synchronization data for installation of the secondary server
INCLUDEPROTECTEDDATAINBACKUP:	True False	
NETWORKTASKDOMAIN:		Used when the Principal (Public) IP addresses are

Tag	Values	Comments
		different for different servers (usually for a DR topology)
NETWORKTASKUSER:		Used when the Principal (Public) IP addresses are different for different servers (usually for a DR topology)
LEAVEONNETWORK:	True False	
COMPUTERNAMEPOSTUNINSTALL:	Must be a string	
CLIENTCONNECTIONPORT:	Must be an integer	
SECONDARYCLONETYPE:	Full Merge Pre clone	**Note:** The Full and Merge clone types are not supported for Command Line Installation
BACKUPUSER:		
SECONDARYPRINCIPLEADDRESS:	Must be an IP address	Only one per line but can be defined multiple times
PRIMARYSECONDARYCHANNEL:	Must be an IP address	Only one per line but can be defined multiple times
STARTSERVICEATEND:	True False	

Command Line Installation of the Primary Server

Installation of SolarWinds Failover Engine begins with the primary server.

1. The following is an example of a parameter file (it must be modified before you use it). <file_name.txt>

   DR Installation Example:

```
INSTALLTYPE:Install
ACCEPT_EULA:true

SERVERROLE:PRIMARY
TOPOLOGY:<DR>
SECONDARYCLONETYPE:"pre clone"
DESTINATIONPATH:"
C:\Program Files\SolarWinds\FoE\
"
PRIMARYSECONDARYCHANNEL:<10.0.1.1,10.0.5.2>
```

```
PRIMARYPRINCIPLEPADDESS:<192.168.99.111>
SECONDARYPRINCIPLEPADDESS:<192.168.98.104>
NETWORKTASKDOMAIN:dnstest.com
NETWORKTASKUSER:administrator
CLIENTCONNECTIONPORT:52267
FEATUREFORINSTALLATION:SolarWinds Failover
  Engine
BACKUPDESTINATIONPATH:\\<10.0.1.1\nf backup>
BACKUPUSER:Administrator
INCLUDEPROTECTEDDATAINBACKUP:true
//AMXPATH:
PLUGINPATH:"C:\nfsql\SqlServerNFPlugin.dll"
//DEFAULTCHANNELPORT:
//BACKUPSOURCEPATH:
STARTSERVICEATEND:True
```

Note: The parameters enclosed in <> must be enclosed in double quotes (") if they contain spaces, dashes or other potentially confusing characters.

2. Download the SolarWinds Failover Engine `.exe` to a suitable location on the primary server and change the file extension from `.exe` to `.zip`.
3. Extract the contents of the SolarWinds Failover Engine `.zip` file into a temporary folder.
4. Navigate to **Start** > **Run** and type `CMD` to open a command window.
5. Navigate to the to the location of the temporary folder.
6. Run the command `:start /wait setup –f:<parameter file> -DNSPassword:<DNS Password> -BACKUPPassword:<backup password> -ni`

Command Line Installation of a Virtual Secondary Server

Installation of the secondary server is similar to installation of the primary server

1. Create a `.txt` file containing the following configuration parameters: This is an example of a parameter file (it must be modified before you use it).

   <file_name.txt>

   ```
   INSTALLTYPE:Install
   SERVERROLE:SECONDARY
   BACKUPSOURCEPATH:\\<192.168.15.111\nf backup>
   BACKUPUSER:Administrator
   ```

   Note: The parameters enclosed in <>must be enclosed in double quotes (") if they contain spaces, dashes or other potentially confusing characters.

2. Download the SolarWinds Failover Engine `.exe` to a suitable location on the secondary server and change the file extension from `.exe` to `.zip`.
3. Extract the contents of the SolarWinds Failover Engine `.zip` file into a temporary folder.
4. Navigate to **Start** > **Run** and type `CMD` to open a command window.
5. Navigate to the to the location of the temporary folder.
6. Run the command: `start /wait setup –f:<parameter file> -BACKUPPassword:<backup password> -ni`

Command Line Installation of a Physical Secondary Server

Installation of the secondary server is similar to installation of the primary server

1. Create a `.txt` file containing the following configuration parameters: This is an example of a parameter file (it must be modified before you use it).

   <file_name.txt>

   ```
   InstallSecParas.txt
   INSTALLTYPE:Install
   SERVERROLE:SECONDARY
   BACKUPSOURCEPATH:\\<192.168.15.111\nf backup>
   BACKUPUSER:Administrator
   ```

   Note: The parameters enclosed in <> must be enclosed in double quotes (") if they contain spaces, dashes or other potentially confusing characters.

2. Download the SolarWinds Failover Engine `.exe` to a suitable location on the secondary server and change the file extension from `.exe` to `.zip`.
3. Extract the contents of the SolarWinds Failover Engine `.zip` file into a temporary folder.
4. Navigate to **Start** > **Run** and type `CMD` to open a command window.
5. Navigate to the to the location of the temporary folder.
6. Run the command: `start /wait setup –f:<parameter file> -BACKUPPassword:<backup password> -ni`

Post Installation Configuration

1. Upon completion of installation, SolarWinds Failover Engine prompts you to activate the SolarWinds Failover Engine license. Enter the Activation key and click **Next**.

Note: If FIPS is enabled, activation of the SolarWinds Failover Engine license may fail. To activate your license on a FIPS enabled server pair, see SWREFID-2255.

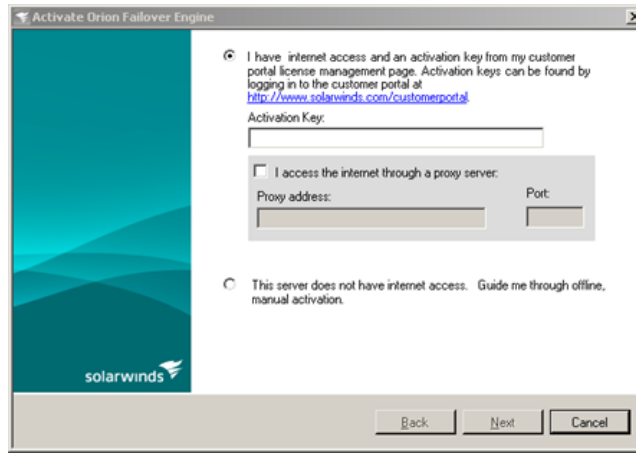
Activate Orion Failover Engine
I have internet access and an activation key from my customer portal license management page. Activation keys can be found by logging in to the customer portal at http://www.solarwinds.com/customerportal.
Activation Key:
I access the internet through a proxy server:
Proxy address:
Port:
This server does not have internet access. Guide me through offline, manual activation.
solarwinds
Back
Next
Cancel

Figure 2: SolarWinds Failover Engine Activation

2. Ensure that the SolarWinds Failover Engine is shut down.
3. Verify that the date, time, and time zone on the secondary server are identical to the same on the primary server.
4. Start the SolarWinds Failover Engine on the primary server.
5. Start the SolarWinds Failover Engine on the secondary server.
6. Right-click the System Tray icon on the primary server and select About SolarWinds Failover Engine to verify v6.7 (11152) is displayed.

Configure actions to take upon failure of a service

SolarWinds Failover Engine assigns three sequential tasks to perform in the event a monitored service fails. Task options include Recover Service, Application Restart, Log Warning, Switchover, and any additional user-defined tasks previously created. By default, SolarWinds Failover Engine assigns Recover Service to each of the three actions. To cause a switchover in the event of service failure, configure the 3rd option to *Switchover*.

Procedure

To configure tasks to perform upon service failure:

1. Using the SolarWinds Failover Manager, navigate to *Applications: Services*.
2. Select the intended service.
3. Click **Edit** and assign a task to each of the three failure options, and then click **OK**.

Important: For dependent services, failure actions must match the failure actions for any protected service on which those services depend, in both type and order. For example:

- Service X is automatically protected by SolarWinds Failover Engine
- Service Y is automatically protected by SolarWinds Failover Engine and has a dependency on service X
- The system administrator sets custom recovery actions for service X as follows:

  First Failure = Recover Service

  Second Failure = Application Restart

  Third Failure = Switchover

  In this situation, the system administrator should also set the service recovery actions for service Y to:

  First Failure = Recover Service

  Second Failure = Application Restart

  Third Failure = Switchover

  Note that if service X fails, the dependent service Y must also fail. If the service recovery actions for service Y are different to those for service X, they may take precedence, for example service X requires a switchover but the failure of service Y has already triggered a service restart action.

This advice applies only to services which are automatically protected by SolarWinds Failover Engine and dependent upon one another. These dependencies may be examined via the Windows Service Control Manager, under **Properties** > **Dependencies**.

For services which are shown in the *Protected services depend on:* pane of the SolarWinds Failover Manager *Applications: Services* page, this advice is not applicable, because:

- These services do not depend on protected services; rather, protected services are dependent upon them; and
- These services are not directly managed by SolarWinds Failover Engine and therefore have no configurable recovery actions.

Note: If an application with the failure option set to *Application Restart* fails, only the services that have failed are restarted. Dependent services do not stop and restart as a result of the failure.

When Additional Pollers (AP)s are not installed, create an Exclusion Filter

To prevent needless replication of temporary files created when Additional Pollers are not used, create an Exclusion Filter.

1. Launch SolarWinds Failover Manger.
2. Navigate to the *Data: File Filters* pane, and click **Add Exclusion Filter** to open the *Add Exclusion Filter* dialog.
3. Type the complete path to or browse to locate the file at the following location:
   - Windows Server 2003: `C:\Documents and Settings\All Users\Application Data\SolarWinds\JobEngine\*.sdf`
   - Windows Server 2008: `C:\ProgramData\Application Data\SolarWinds\JobEngine\*.sdf`
   - Windows Server 2012: `C:\ProgramData\Application Data\SolarWinds\JobEngine\*.sdf`
4. click **OK**.

When IPAM 2.0 is installed, create an Inclusion Filter

To create the Inclusion Filter:

1. Launch the SolarWinds Failover Manager on the active server.
2. Navigate to *Data: File Filters*.
3. Click **Add Inclusion Filter**.
4. Type the path below or browse to the file location.
   `<installation_dir>\Orion\Information Service\2.0\Schemas\IPAM.attributes.xml`
5. Click **OK**.

Command Line Installation of SolarWinds Failover Engine Client Tools

SolarWinds Failover Engine allows installation of SolarWinds Failover Engine Client Tools for remote management of SolarWinds Failover Engine clusters.

Prerequisites

When installing SolarWinds Failover Engine Client Tools on Windows XP, the following Service Pack levels are required.

- Windows XP 32 bit SP3
- Windows XP 64 bit SP2

1. Create a `.txt` file containing the following configuration parameters:

   Important: The following is an example of a parameter file (it must be modified before you use it). The content within the characters < and > indicate example text and the actual < and > characters should not be present in the edited file.

   ```
   INSTALLTYPE:"Install Client Tools Only"

   ACCEPT EULA:true

   DESTINATIONPATH:<C:\AutoInstall>
   ```

2. Download the SolarWinds Failover Engine `.exe` to a suitable location on the workstation and change the file extension from `.exe` to `.zip`.
3. Extract the contents of the SolarWinds Failover Engine `.zip` file into a temporary folder.
4. Navigate to **Start > Run** and type `CMD` to open a DOS window.
5. Navigate to the to the location of the temporary folder.
6. Run the command: `start /wait setup -f:<parameter file> -ni`
7. Upon completion of the unattended installation, the **Manage Server** icon will appear on the desktop.

Command Line Uninstall of SolarWinds Failover Engine

SolarWinds Failover Engine allows you to uninstall the product from your Server using the command line method.

1. Ensure all the SolarWinds Failover Engine processes are stopped and close the SolarWinds Failover Manager and System Tray icon.
2. Create a `.txt` file with the following configuration parameters:

   Important: The following is an example of a parameter file (it must be modified before you use it). The content within the characters < and > indicate example text and the actual < and > characters should not be present in the edited file.

   ```
   INSTALLTYPE:Uninstall

   LEAVEONNETWORK:true
   ```

3. Navigate to the SolarWinds Failover Engine `.exe` file and change the file extension from `.exe` to `.zip`.
4. Extract the contents of the SolarWinds Failover Engine `.zip` file into a temporary folder.

5. Navigate to **Start > Run** and type `CMD` to open a DOS window.
6. Navigate to the to the location of the temporary folder.
7. Run the command: `start /wait setup –f:<parameter file> -ni`

   After the uninstall process completes, you will be notified of any files that could not be removed and advised to delete them manually.

   Note: The `SupportLogs` directory is also left behind. This is intentional and should not be deleted in the event you need to submit a support report.

Appendix A

Setup Error Messages

The following table provides a listing of the most common error messages displayed during setup.

Table 4: Setup Error Messages

Message	Pri	Sec	Level	Test
10 – 'The pre install check data file does not have the correct format. Setup cannot continue'.	No	Yes	Critical Stop	Check that the file adheres to the correct formatting and structure for use in analysis on the secondary.
Setup has detected incompatible versions of the collector version $x and the analyzer version $y dll. This would suggest different versions of Setup have been run on the Primary and Secondary servers.	No	Yes	Critical Stop	Check that the analyzer and collector dlls are compatible.
File $x cannot be analyzed it may be corrupt Setup is unable to continue. If the file has been opened check that it has not been saved with Word Wrap.	–	Yes	Critical Stop	Check file format is correct.
190 – This server is a #1# domain controller. SolarWinds Failover Engine must not be installed on a domain controller.	Yes	Yes	Critical Stop	Test whether the server is a domain controller.
173 – SolarWinds Failover Engine does not support the '/3GB'	Yes	Yes	Critical Stop	Test for /3GB on Windows 2000

Message	Pri	Sec	Level	Test
switch on Windows 2000 Standard Edition.				
175 – SolarWinds Failover Engine requires Windows 2003 Standard Edition SP1 or later if '/3GB' switch is on.	Yes	Yes	Critical Stop	
103 - SolarWinds Failover Engine does not support #1#. The following are supported Windows 2000 Server SP4 or greater; Windows Server 2003 SP1 or greater.	Yes	Yes	Warning	
200 - Your #1# server uses the Intel ICH7 chipset and Windows 2000 has been detected. This combination is incompatible with SolarWinds Failover Engine.	Yes	Yes	Critical Stop	
217 - SolarWinds Failover Engine is not supported on Windows Storage Server Edition.	Yes	Yes	Warning	
106 - Primary and Secondary OS versions are not identical, #1# vs. #2#: and require the same Service Pack level.	–	Yes	Critical Stop	Compatibility check on secondary.
208 - You are running a 64-bit version of Windows on one of your servers and a 32-bit version of Windows on	–	Yes	Critical Stop	Compatibility check on secondary.

Message	Pri	Sec	Level	Test
the other. This is not supported.				
111 - The system folders on primary and secondary system must be the same. Setup has detected that the secondary system folder is #2# and the primary was #1#.	–	Yes	Critical Stop	Compatibility check on secondary.
113 - You do not have enough total memory to install SolarWinds Failover Engine on your #1# server. You must have at least 1GB.	Yes	Yes	Critical Stop	
SolarWinds recommends a minimum of 2GB. Note actual memory requirements depend on the application load; and may require more memory.	Yes	Yes	Warning	
117 - You do not have enough free disk space to install SolarWinds Failover Engine You must have at least 2GB available.	Yes	Yes	Critical Stop	
118 - For every volume on the primary system that contains protected data a corresponding volume must exist on the secondary server. In most cases this means that for every volume on the primary server a volume with the same drive letter	–	Yes	Warning	Compatibility check on secondary.

Message	Pri	Sec	Level	Test
(such as D:\) must exist on the secondary server. If this is not the case, the secondary server must be modified to meet this requirement.				
204 - Your operating system on your #1# server is #2# and you are running with a Windows 2000 driver for your NC77xx NIC(s). In order to prevent system crashes you must upgrade to a Windows 2003 driver; the name for those drivers ends with '57XP32.sys' and not with '57W2K.sys'	Yes	Yes	Critical Stop	
212 - The number of Free System Page Table Entries on this server has dropped to #1#. This is too low. You should have at least #2# Free System Page Table Entries available.	Yes	Yes	Critical Stop	
201 - #1#: This service is incompatible with running SolarWinds Failover Engine and must be stopped before SolarWinds Failover Engine can be installed.	Yes	Yes	Warning	
209 - Double-Take drivers have been detected on this	Yes	Yes	Critical Stop	

Message	Pri	Sec	Level	Test
server. To avoid compatibility problems please uninstall Double-Take before re-running setup.				

Appendix B

Installation Verification Testing

Installation Verification testing is a procedure performed to validate the configuration of the server Cluster and its performance after installation.

Testing a SolarWinds Failover Engine Pair

Important: The following procedure provides information about performing Installation Verification testing on a SolarWinds Failover Engine pair to ensure proper installation and configuration. Additionally, this procedure provides step-by-step procedures to perform a controlled switchover in the event of an application failure and failover in the event of network or hardware failure resulting in excessive missed heartbeats.

Note: In this document, the term “Pair” refers to a SolarWinds Failover Engine pair. Refer to the for more information about SolarWinds Failover Engine Pairs.

Exercise 1 - Auto-switchover

SolarWinds Failover Engine monitors SolarWinds services and the system environment to ensure that protected services are available for end users. To monitor services and the system environment, SolarWinds Failover Engine uses plug-ins which are designed for SolarWinds services and the system.

If a protected service or the system begins to operate outside of preconfigured thresholds, SolarWinds Failover Engine can automatically switch to make the passive server the active server in the pair that provides services for end users.

Important: These exercises are examples and should be performed in order. SolarWinds recommends against attempting to test failover on a properly operating pair by methods such as unplugging a power cord. At the moment power is lost, any data not written to the passive server is lost. SolarWinds recommends that all actions intended to verify operation of the passive server be performed as a switchover rather than a failover.

Starting Configuration

Prior to initiating the Installation Verification process in a pair, SolarWinds Failover Engine must be configured with the primary server as active and the secondary server as passive. Additionally, the following prerequisites must be met:

- The secondary server must be synchronized with the primary server.
- All protected services must be operating normally.

- If installed in a LAN environment, verify that *Failover from Primary server to Secondary server if channel heartbeat is lost for failover timeout* is selected from the **Server: Monitoring** > **Configure Failover** dialog (default setting).
- If installed in a WAN environment, you must manually select *Failover from Primary server to Secondary server if channel heartbeat is lost for failover timeout* in the **Server: Monitoring** > **Configure Failover** dialog.

Important: Prior to starting the Installation Verification process, ensure that a known good backup of the primary server exists and examine the Windows event logs for recent critical errors.

SolarWinds provides an executable, `nfavt.exe`, to emulate conditions that result in auto-switchover so you can verify that your SolarWinds Failover Engine installation performs as expected. This section guides you through the steps necessary to perform this verification.

Steps to Perform

Important: If you encounter errors and or find it necessary to back out the changes made by this exercise, you can stop at any point and perform the steps described in the *Back-out Procedure (Auto-switchover)* to return the Pair to its original operating configuration and state.

Table 5: Perform the following procedure to verify Auto-Switchover in a Pair configuration.

Machine ID	Activity	Results
primary	Open a command prompt.	
	Change directory to `C:\Program Files\SolarWinds\FoE\r2\Bin`	
	Execute `nfavt.exe` When prompted, "*Are you sure you wish to continue*", click **Continue**.	Service is switched to the secondary server and SolarWinds Failover Engine shuts down on the primary.
secondary	Login to the SolarWinds Failover Manager.	
	In the *Servers* pane of the SolarWinds Failover Manager, select the server pair.	The *System Overview* screen indicates that the secondary server is active.
	Verify all protected applications have started on the secondary.	Services are running on the secondary.

Machine ID	Activity	Results
	Verify data is present.	Data is present.

Successful completion of this procedure leaves the SolarWinds Failover Engine pair in the state necessary to perform the second part of the Installation Verification process, detailed in *Exercise 2 - Data Verification*.

Back-out Procedure (Auto-switchover)

Important: Do not perform this back-out procedure if you intend to continue the Installation Verification process.

If for any reason you find it necessary to back out of this exercise, you can stop at any point and return the pair to the state it was in at the beginning of this exercise by performing the following steps:

1. Shut down SolarWinds Failover Engine and protected services on all servers.
2. Complete the following on both servers:
    a. Open the *Configure Server* wizard.
    b. Select the *Machine* tab.
    c. Select the *Primary* server as active.
    d. Click **Finish**.
3. On the secondary server, right-click the taskbar icon and select *Start SolarWinds Failover Engine* .
4. Verify that the secondary server is passive (**S/–**).
5. On the primary server, right-click the taskbar icon and select *Start SolarWinds Failover Engine* .
6. After SolarWinds Failover Engine starts, login to the SolarWinds Failover Manager.
7. Verify that applications have started and replication to the passive server has resumed.

Exercise 2 - Data Verification

The Data Verification exercise validates that data is synchronized between the servers resulting in current data on the active server following the Auto-switchover exercise performed previously. The objective is to take a working active server (the secondary server) and synchronize it with the passive (primary server). This exercise also demonstrates that all the correct services stopped when the primary server became passive.

Starting Configuration

SolarWinds Failover Engine is running on the secondary active server. Using the *System Tray* icon, verify that the server status displays **S/A**. SolarWinds Failover Engine is not running on the primary server which is set to passive. Using the *System Tray* icon, verify that the server status displays **-/-** to indicate that SolarWinds Failover Engine is not running.

Steps to Perform

Table 6: Perform the following steps to verify that data is synchronized following Auto-switchover in a Pair configuration.

Machine ID	Activity	Results
primary	Right-click the taskbar icon and select *Start SolarWinds Failover Engine* .	SolarWinds Failover Engine successfully starts.
	Login to SolarWinds Failover Manager.	
	In the *Servers* pane of the SolarWinds Failover Manager, select the server pair.	The *System Overview* screen is displayed.
	Navigate to the *Server: Summary* tab to show the connection from the secondary (active) to primary (passive).	The *Server: Summary* page shows a connection from the secondary server to the primary server.
	Select the *Data: Replication* tab and wait for both the *File System* and the *Registry* status to display as *Synchronized*. Access the SolarWinds Failover Engine logs and confirm that no exception errors occurred during the synchronization process.	Data replication resumes from the secondary server back to the primary server. Both the *File System* & *Registry* status become *Synchronized*.

Successful completion of this procedure leaves the SolarWinds Failover Engine Pair in the state necessary to perform the final part of the Installation Verification process, detailed in *Exercise 3 - Switchover*.

Exercise 3 - Switchover

The Switchover exercise demonstrates the ability to switch the functionality and operations of the active server on command to the other server in the pair using the SolarWinds Failover Engine. Perform this exercise only after successfully completing the Auto-switchover and Data Verification Exercises.

Starting Configuration

SolarWinds Failover Engine is running on the secondary active server. Using the *System Tray* icon, verify that the server status displays **S/A**. SolarWinds Failover Engine is running on the primary server which is set to passive. Using the *System Tray* icon, verify that the server status displays **P/-** to indicate that SolarWinds Failover Engine is running on the primary server and that the primary server is passive

Steps to Perform

Table 7: Perform the following steps to switch functionality and operations on command from the active server to the ready standby server.

Machine ID	Activity	Results
secondary	Launch SolarWinds Failover Manager and select the *Data: Replication* tab. Verify that both the *File System* and I status are *Synchronized*.	
	Select the *Server: Summary* tab. Select the primary server icon and click **Make Active**.	The SolarWinds Failover Manager *Server: Summary* page displays the applications stopping on the active server. Once all applications are stopped, the active server becomes passive and the passive server becomes active. The Console shows the applications starting on the newly active server. Both the *File System* and *Registry* status are *Synchronized*.
	Confirm application performance and availability meets previously defined criteria. Verify that client applications are running as expected after the switchover process.	Services continue to be provided as before the switchover occurred. You may need to refresh or restart some client applications as a result of a switchover.

Successful completion of this procedure indicates a successful outcome from the Installation Verification process.

Glossary

Active
The functional state or role of a server when it is visible to clients through the network, running protected applications, and servicing client requests.

Alert
A notification provided by SolarWinds Failover Engine sent to a user or entered into the system log indicating an exceeded threshold.

Active Directory (AD)
Presents applications with a single, simplified set of interfaces so users can locate and use directory resources from a variety of networks while bypassing differences between proprietary services. SolarWinds Failover Engine switchovers and failovers require no changes to AD resulting in switchover/failover times typically measured in seconds.

Active–Passive
The coupling of two servers with one server visible to clients on a network and providing application service while the other server is not visible and not providing application service to clients.

Active Server Queue
The staging area of the active server used to store intercepted data changes before being transported across the channel to the passive server.

Advanced Configuration and Power Interface (ACPI)
A specification that dictates how the operating system can interact with the hardware especially where power saving schemes are used. The primary and secondary servers must have identical ACPI compliance.

Asynchronous
A process whereby replicated data is applied (written) to the passive server independently of the active server.

Basic Input/Output System (BIOS)
The program a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.

Cached Credentials
Locally stored security access credentials used to log into a computer system when a Domain Controller is not available.

Channel Drop
An event in which the dedicated communications link between servers fails, often resulting in the passive server becoming active and consequently creating a split-brain syndrome.

Channel NIC (Network Interface Card)
A dedicated subnet used by the SolarWinds Channel.

Checked
The status reported for user account credential (username/password) validation.

Cloned Servers
Servers that have identical configuration settings, names, applications, Security Identifiers (SIDs) and IP addresses, following the installation of SolarWinds Failover Engine.

Cloning Process
The SolarWinds Failover Engine process whereby all installed programs, configuration settings, and the machine name, Security Identifier (SID), and IP address are copied to another server.

Cluster
A generic term for SolarWinds Failover Engine Pair and the set of machines (physical or virtual) involved in supporting a single protected server. SolarWinds Failover Engine Cluster can include the machines used in a VMware or Microsoft cluster.

Connection
Also referred to as Cluster Connection. Allows the SolarWinds Failover Manager to communicate with SolarWinds Failover Engine Cluster, either on the same machine or remotely.

Crossover Cable
A network cable that crosses the transmit and receive lines.

Data Replication
The transmission of protected data changes (files and registry) from the active to the passive server via the SolarWinds Channel.

Data Rollback Module
SolarWinds Failover Engine module that allows administrators to rollback the entire state of a protected application, including files and registry settings, to an earlier point-in-time. Typically used after some form of data loss or corruption.

Degraded
The status reported for an application or service that has experienced an issue that triggered a Rule.

Device Driver
A program that controls a hardware device and links it to the operating system.

Disaster Recovery (DR)
A term indicating how you maintain and recover data with SolarWinds Failover Engine in event of a disaster such as a hurricane or fire. DR protection can be achieved by placing the secondary server at an offsite facility, and replicating the data through a WAN link.

DNS (Domain Name System) Server
Provides a centralized resource for clients to resolve NetBIOS names to IP addresses.

Domain
A logical grouping of client server based machines where the administration of rights across the network are maintained in a centralized resource called a domain controller.

Domain Controller (DC)
The server responsible for maintaining privileges to domain resources; sometimes called AD controller in Windows 2003 and above domains.

Dualed
A way to provide higher reliability by dedicating more than one NIC for the SolarWinds Channel on each server.

Failover
Failover is the process by which the first passive server assumes the active role when it no longer detects that the active server is alive as a result of a critical unexpected outage or crash of a server.

Full System Check (FSC)
The internal process automatically started at the initial connection or manually triggered through the Manage Server GUI to perform verification on the files and registry keys and then synchronize the differences.

Fully Qualified Domain Name (FQDN)
Also known as an absolute domain name, a FQDN specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain, relative to the root domain. Example: somehost.example.com., where the trailing dot indicates the root domain.

Global Catalog
A global catalog is a domain controller that stores a copy of all Active Directory objects in a forest. The global catalog stores a full copy of all objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest.

Graceful (Clean) Shutdown
A shutdown of SolarWinds Failover Engine based upon completion of replication by use of the SolarWinds Failover Engine SolarWinds Failover Manager, resulting in no data loss.

Group
An arbitrary collection of SolarWinds Failover Engine Clusters used for organization.

Hardware Agnostic
A key SolarWinds Failover Engine feature allowing for the use of servers with different manufacturers, models, and processing power in a single SolarWinds Failover Engine Cluster.

Heartbeat
The packet of information issued by the passive server across the channel, which the active server responds to indicating its presence.

High Availability (HA)
Keeping users seamlessly connected to their applications regardless of the nature of a failure. LAN environments are ideally suited for HA.

Hotfix
A single, cumulative package that includes one or more files that are used to address a problem in a product.

Identity
The position of a given server in the SolarWinds Failover Engine Cluster: primary or secondary.

Install Clone
The installation technique used by SolarWinds Failover Engine to create a replica of the primary server using NTBackup or Wbadmin and to restore the replica to the secondary server.

Low Bandwidth Module (LBM)
SolarWinds Failover Engine module that compresses and optimizes data replicated between servers over a WAN connection. This delivers maximum data throughput and improves application response time on congested WAN links.

Machine Name
The Windows or NETBIOS name of a computer.

Management IP Address
An additionally assigned unfiltered IP address used for server management purposes only.

Many-to-One
The ability of one physical server (hosting more than one virtual server) to protect multiple physical servers.

Network Monitoring
Monitoring the ability of the active server to communicate with the rest of the network by polling defined nodes across the network at regular intervals.

Pair
See SolarWinds Failover Engine Pair above.

Passive
The functional state or role of a server when it is not delivering service to clients and is hidden from the rest of the network.

Passive Server Queue
The staging area on the passive server used to store changes received from the active server before they are applied to the disk/registry on the passive server.

Pathping
A route-tracing tool that works by sending packets to each router on the way to a final destination and displays the results of each hop.

Plug-and-Play (PnP)
A standard for peripheral expansion on a PC. On starting the computer, PnP automatically configures the necessary IRQ, DMA and I/O address settings for the attached peripheral devices.

Plug-in
An application specific module that adds SolarWinds Failover Engine protection for the specific application.

Pre-Clone
An installation technique whereby the user creates an exact replica of the primary server using VMware vCenter Converter or other 3rd party utility prior to the initiation of installation and uses the replica as a secondary server.

Pre-Installation Checks
A set of system and environmental checks performed as a prerequisite to the installation of SolarWinds Failover Engine.

Primary
An identity assigned to a server during the SolarWinds Failover Engine installation process that normally does not change during the life of the server and usually represents the production server prior to installation of SolarWinds Failover Engine.

Principal (Public) IP Address
An IP address used by clients to contact the server through drive mappings, UNC paths, DNS resolved paths, etc. to gain access to the server's services and resources.

Principal NIC
The network card which hosts the Principal IP address.

Principal (Public) Network
The network used by clients to connect to server applications protected by SolarWinds Failover Engine.

Protected Application
An application protected by the SolarWinds Failover Engine solution.

Quality of Service (QoS)
An effort to provide different prioritization levels for different types of traffic over a network. For example, SolarWinds Failover Engine data replication may have a higher priority than ICMP traffic, as the consequences of interrupting data replication are more obvious than slowing down ICMP traffic.

Receive Queue
The staging area on a server used to store changes received from another server in the replication chain before they are applied to the disk/registry on the passive server.

Remote Desktop Protocol (RDP)
A multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services.

Replication
The generic term given to the process of intercepting changes to data files and registry keys, transporting the changed data across the channel, and applying them to the passive server(s) so the servers are maintained in a synchronized state.

Role
The functional state of a server in the SolarWinds Failover Engine Cluster: active or passive.

Rule
A set of actions performed by SolarWinds Failover Engine when defined conditions are met.

Secondary
An identity assigned to a server during the SolarWinds Failover Engine installation process that normally does not change during the life of the server and usually represents the standby server prior to installation of SolarWinds Failover Engine.

Security Identifier (SID)
A unique alphanumeric character string that identifies each operating system and each user in a network of 2003/2008/2012 systems.

Send Queue
The staging area on a server used to store intercepted data changes before being transported across to a passive server in the replication chain.

Server Monitoring
Monitoring of the active server by the passive server, using a heartbeat message, to ensure that the active server is functional.

Shared Nothing
A key feature of SolarWinds Failover Engine in which no hardware is shared between the primary or secondary server. This prevents a single point of failure.

SMTP
A TCP/IP protocol used in sending and receiving e-mail between servers.

SNMP
Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks.

SolarWinds Channel
The IP communications link used by the SolarWinds Failover Engine system for the heartbeat and replication traffic.

SolarWinds Failover Engine
The core replication and system monitoring component of the SolarWinds Failover Engine solution.

SolarWinds Failover Engine Diagnostics

The umbrella name for the SolarWinds Failover Engine process and tools used to verify the production servers health and suitability for the implementation of a SolarWinds Failover Engine solution.

SolarWinds Failover Engine Heartbeat Packet Filter

The network component, installed on all servers, that controls network visibility.

SolarWinds Failover Engine Pair

Describes the coupling of the primary and secondary server in a SolarWinds Failover Engine solution.

SolarWinds Failover Engine Plug-ins

Optional modules installed into a SolarWinds Failover Engine server to provide additional protection for specific applications.

SolarWinds Failover Engine Switchover/Failover Process

A process unique to SolarWinds Failover Engine in which the passive server gracefully (switchover) or unexpectedly (failover) assumes the role of the active server providing application services to connected clients.

Split-Brain Avoidance

A unique feature of SolarWinds Failover Engine that prevents a scenario in which primary and secondary servers attempt to become active at the same time leading to an active-active rather than an active-passive model.

Split-Brain Syndrome

A situation in which more than one server in SolarWinds Failover Engine Cluster are operating in the active mode and attempting to service clients, resulting in the independent application of different data updates to each server.

Subnet

Division of a network into an interconnected but independent segment or domain, intended to improve performance and security.

Storage Area Network (SAN)

A high-speed special-purpose network or (subnetwork) that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users.

Switchover

The graceful transfer of control and application service to the passive server.

Synchronize

The internal process of transporting 64KB blocks of changed files or registry key data, through the SolarWinds Channel, from the active server to the first

passive server or from the first passive server to the second passive server to ensure the data on the passive server is a mirror image of the protected data on the active server.

System Center Operations Manager (SCOM)

System Center Operations Manager is a cross-platform data center management server for operating systems and hypervisors.

System State

Data that comprises the registry, COM+ Class Registration database, files under Windows File Protection, and system boot file; other data may be included in the system state data.

Task

An action performed by SolarWinds Failover Engine when defined conditions are met.

Time-To-Live (TTL)

The length of time that a locally cached DNS resolution is valid. The DNS server must be re-queried after the TTL expires.

Traceroute

A utility that records the route through the Internet between your computer and a specified destination computer.

Ungraceful (Unclean) Shutdown

A shutdown of SolarWinds Failover Engine resulting from a critical failure or by shutting down Windows without first performing a proper shutdown of SolarWinds Failover Engine, resulting in possible data loss.

Unprotected Application

An application not monitored nor its data replicated by SolarWinds Failover Engine.

Virtual Private Network (VPN)

A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Windows Management Instrumentation (WMI)

A management technology allowing scripts to monitor and control managed resources throughout the network. Resources include hard drives, file systems, operating system settings, processes, services, shares, registry settings, networking components, event logs, users, clusters, and groups.